# Geometric Characterization of Quantum Oracle Identification(New Trends in Theory of Computation and Algorithm)

AUTHOR(S):

Kawachi, Akinori; Yamashita, Shigeru

数理解析研究所講究録
1489 巻 2006 年 121-127



# Geometric Characterization of Quantum Oracle Identification

Akinori Kawachi *
(河内 亮周)

Shigeru Yamashita †
(山下 茂)

**Abstract—** We geometrically characterize the query complexity of the oracle identification problem in this paper. By defining an inner product between two oracles, we construct a quantum algorithm, which generalizes Bernstein-Vazirani and Grover algorithms, for a certain class of the oracle identification problem characterized by the inner product. We also show the optimality of this quantum algorithm.

**Keywords:** quantum algorithms, query complexity, oracle identification problem

## 1 Introduction

The oracle identification problem (OIP) introduced by Ambainis et al. [1] is a general framework for the quantum oracle computation, which generalizes many important instances such as the equivalence problem (EQ) [4], and the inner product problem (IP) [3]. The formal definition of OIP is given as follows.

**Oracle Identification Problem (OIP)**
**Input:** a set $S = \{f_i | f_i : \{0, ..., N-1\} \to \{0, 1\}, i = 0, ..., M-1\}$ of oracles and a black-box oracle $f_k \in S$.
**Output:** $k$.

The general upper bounds for an arbitrary OIP are given in [1, 2]. However, actual query complexity of OIP depends on a special structure of instances. For example, the query complexities of IP and EQ are respectively 1 and $O(\sqrt{N})$, as shown in [3, 4]. As seen in EQ and IP, we have a large gap among OIPs on their query

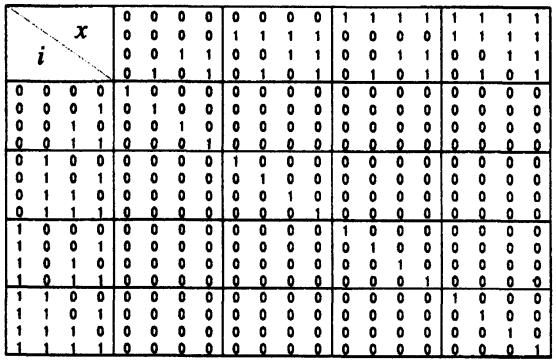

Figure 1: EQ oracle

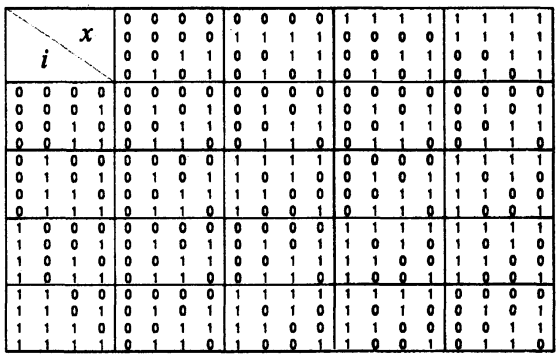

Figure 2: IP oracle

complexities. What causes such a large gap of their query complexities? Let us see Figs. 1 and 2. One can guess that an EQ oracle is so "close" to each other that we need to many queries to distinguish them, and an IP oracle is the contrary. Now, we translate their values 0 and 1 into +1 and −1. We can then formulate the "closeness" as the inner product between every two rows (i.e., two oracles). One can see easily that the inner product of two distinct row vectors is orthogonal in IP and that takes a large value in EQ. This "closeness" seems to characterize their query complexities. More formally, we now introduce a notion of the *oracle state*.

* Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan. kawachi@is.titech.ac.jp.

† Graduate School of Information Science, Nara Institute of Science and Technology. 8916-5, Takayama-cho Ikoma-shi, Nara 630-0192, Japan. ger@is.naist.jp

**Definition 1.1** For an oracle $f : \{0,1\}^n \to \{0,1\}$, an oracle state of $f$ is defined as

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i\rangle.$$

By this notion, we also define an inner product $\langle f|g\rangle$ between two oracles $f$ and $g$.

In this paper, we geometrically characterize the query complexities of a certain class including the important instances using the notion of the oracle state. Our first result is to characterize the upper bounds of the query complexities by the inner product between oracles for a special case of OIP including IP and EQ. More precisely, we give a quantum algorithm for any OIP $S = \{f_0, ..., f_{N-1}\}$ satisfying $c\sigma \le \langle f_k|f_l\rangle \le \sigma$ for any distinct $k$ and $l$ and any constant $0 < c < 1$ using $O((1 - |\sigma|)^{-1/2})$ queries with a constant probability.

It is straightforward that $\sigma = 1 - (4/N)$ in the case of the EQ oracles and $\sigma = 0$ in the case of the IP oracles. Substituting these values to the above statement, their query complexities correspond to the original ones up to a constant.

We also present the optimality of our quantum algorithms, i.e., we show that there exists an OIP that needs $\Omega(1/\sqrt{1 - \sigma_{max}})$, where $\sigma_{max} = \max_{i \neq j} |\langle f_i|f_j\rangle|$.

## 2 Upper Bounds

To show the upper bounds for OIP, we will construct quantum algorithms whose query complexity depends on the orthogonality of oracle states.

First, we describe our idea for their constructions based on geometrical intuitions. Suppose that we are given an oracle state $|f_k\rangle$ in $\{|f_0\rangle, ..., |f_{N-1}\rangle\}$ rather than an oracle $f_k$. We then try to identify $|f_k\rangle$ by applying a unitary operator $U = (|u_0\rangle \cdots |u_{N-1}\rangle)^\dagger$, where $\{|u_i\rangle\}_i$ is an $N$-dimensional orthonormal basis. Then, the probability obtaining $|k\rangle$ by measuring $U|f_k\rangle$, i.e., the success probability, is $|\langle u_k|f_k\rangle|^2$. Hence, our task is to construct the optimal orthonormal basis maximizing the success probability for all $k$.

Actually, since we are given an oracle $f_k$, we might be able to amplify the success probability by approaching the original oracle state $|f_k\rangle$ to a quantum state $|f'_k\rangle$ close to $|u_k\rangle$ via queries to $f_k$. We can then find $|k\rangle$ with high probability, $|\langle u_k|f'_k\rangle|^2$, by measuring $U|f'_k\rangle$.

Therefore, we consider the following two steps to construct quantum algorithms for OIP: (i) We find the $N$-dimensional orthonormal basis $\{u_i\}_i$ and (ii) construct quantum operations that approaches $|f_k\rangle$ to $|f'_k\rangle$.

### 2.1 Equiangular Case

For simplicity, we now consider a case of every pair of oracle states having an identical value $\sigma \ge 0$ of the inner product, i.e., for any distinct two oracles $f_k, f_l$, $\langle f_k|f_l\rangle = \sigma \ge 0$.

**Equiangular Oracle Identification Problem (EOIP)**
**Input:** a set $S = \{f_0, ..., f_{N-1}\}$ of $N$ oracles, a black-box oracle $f_k \in S$.
**Promise:** $\langle f_i|f_j\rangle = \sigma \ge 0$ for any distinct $i$ and $j$.*
**Output:** $k$.

We define the query complexity of EOIP as the number of queries to identify oracles in the worst-case with at least a constant probability. We stress that this special case already includes significant instances such as OIPs for the EQ oracle and the IP oracle.

First, we find the $N$-dimensional orthonormal basis $\{u_i\}_i$, equivalently a unitary operator $U$, to maximize the success probability that every oracle state $|f_k\rangle$ can be identified, as stated above. The intuition of our construction for $U$ is simple in this case. If oracle states are orthonormal, we directly define a unitary operator $U$ as enumeration of oracle states: $U = (|f_0\rangle \cdots |f_{N-1}\rangle)^\dagger$. Otherwise, we need to adjust the oracle states $\{|f_i\rangle\}_i$ to othonormal states

* We can assume $\sigma \ge 0$ without loss of generality by fliping all outputs of an oracle if $\sigma < 0$.

$\{|u_i\rangle\}_i$. To maximize the success probability that we identify every oracle state, we *open up* the oracle states around the *mean* state $|c\rangle$ among $\{|f_i\rangle\}_i$ as preserving the equiangularity among the oracle states. (Fig. 3.) Then, we can obtain the orthonormal states $\{|u_i\rangle\}_i$ such that $u_i$ is on the plane spanned by $|f_i\rangle$ and $|c\rangle$ for every $i$. Here, the mean state is formally given as follows.

**Definition 2.1** The mean state $|c\rangle$ for OIP $S = (f_0, ..., f_{N-1})$ is defined as

$$|c\rangle = \frac{1}{\| \sum_{i=0}^{N-1} |f_i\rangle \|} \sum_{i=0}^{N-1} |f_i\rangle.$$

Now let

$$\langle f_k|c\rangle = \cos\theta, \qquad \langle u_k|f_k\rangle = \cos\phi$$

for any $k \in \{0, ..., N-1\}$.

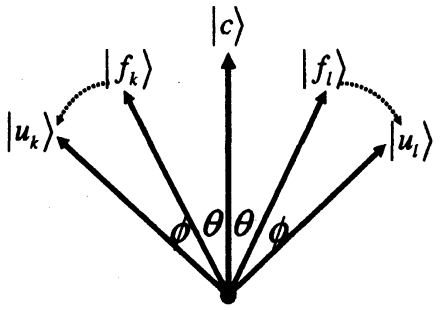


Figure 3: Construction of $U$

In the case of EOIP, we can represent the inner products $\langle u_k|f_k\rangle$ and $\langle f_k|c\rangle$ with $\sigma$, which are used for analysis of our algorithm.

**Lemma 2.2** For the orthonomal states $|u_0\rangle, ..., |u_{N-1}\rangle$ we have

$$\langle u_k|f_k\rangle = \cos\phi = \frac{1}{N}\sqrt{\sigma(N-1)+1} + \left(1 - \frac{1}{N}\right)\sqrt{1-\sigma} = \Theta(\sqrt{1-\sigma})$$

and

$$\langle f_k|c\rangle = \cos\theta = \sqrt{\frac{1+\sigma(N-1)}{N}} = \Theta(\sqrt{\sigma})$$

for any $k \in \{0, ..., N-1\}$

**Proof.** For any distinct two oracles $f_k, f_l$, if $\langle f_k|f_l\rangle = \sigma \geq 0$,

$$|c\rangle = \frac{1}{\sqrt{N + \sigma(N^2 - N)}} \sum_{i=0}^{N-1} |f_i\rangle$$

since

$$\left\| \sum_{i=0}^{N-1} |f_i\rangle \right\| = \sqrt{\sum_{i,j} \langle f_i|f_j\rangle} = \sqrt{N + \sigma(N^2 - N)}.$$

We therefore obtain

$$\begin{aligned} \langle f_k|c\rangle &= \cos\theta = \sqrt{\frac{1+\sigma(N-1)}{N}}, \\ \langle u_k|c\rangle &= \cos(\theta+\phi) = \frac{1}{\sqrt{N}}. \end{aligned}$$

Note that $\theta, \phi > 0$ and $\theta + \phi < \pi/2$. We have

$$\begin{aligned}
\cos\phi &= \cos(\phi + \theta - \theta) \\
&= \cos\theta\cos(\phi+\theta) + \sin\theta\sin(\phi+\theta) \\
&= \cos\theta\cos(\phi+\theta) + \sqrt{1-\cos^2\theta}\sqrt{1-\cos^2(\phi+\theta)} \\
&= \sqrt{\frac{1+\sigma(N-1)}{N}}\frac{1}{\sqrt{N}} + \sqrt{\left(1-\frac{1}{N}\right)(1-\sigma)}\sqrt{1-\frac{1}{N}} \\
&= \frac{1}{N}\sqrt{\sigma(N-1)+1} + \left(1-\frac{1}{N}\right)\sqrt{1-\sigma}.
\end{aligned}$$

□

Now, we give the upper bounds of any EOIP in the following theorem.

**Theorem 2.3** There exists a quantum algorithm that solves any EOIP using at most $O\left((1-\sigma)^{-1/2}\right)$ queries with probability at least $\Omega(\max\{\sigma, 1-\sigma\})$.

**Proof.** As stated in the previous section, we have to construct a procedure for approaching the oracle state $|f_k\rangle$ to the base state $|u_k\rangle$ by queries to $f_k$. For this purpose, we incorporate a geometrical implication of the Grover search [4, 5] into our algorithm and generalize it for our problem. More specifically, we make use of the following two reflection operators:

$$R_c = 2|c\rangle\langle c| - I, \qquad R_{f_k} = 2|f_k\rangle\langle f_k| - I.$$

One can easily see that a reflection operator with respect to a state $|\psi\rangle$ "reflects" any state across $|\psi\rangle$. Note that we can construct $R_c$ with no queries to $f_k$ and $R_{f_k}$ with two queries since

$$R_{f_k} = O_{f_k}(2|0\rangle\langle 0| - I)O_{f_k}^{\dagger},$$

where $O_{f_k}$ is a unitary operator satisfying

$$O_{f_k}|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}(-1)^{f_k(x)}|x\rangle$$

which can be constructed with a single query to $f_k$.

Recall that $\cos\theta = \langle f_k|c\rangle$ and $\cos(\phi+\theta) = \langle u_k|c\rangle$. Since we have $0 < \theta < \theta + \phi < \pi/2$ and $|f_k\rangle, |u_k\rangle$ and $|c\rangle$ are on the same plane, we can approach $|f_k\rangle$ to $|u_k\rangle$ by repeating applications of $R_c$ and $R_{f_k}$ to $|f_k\rangle$, as shown Fig. 4.

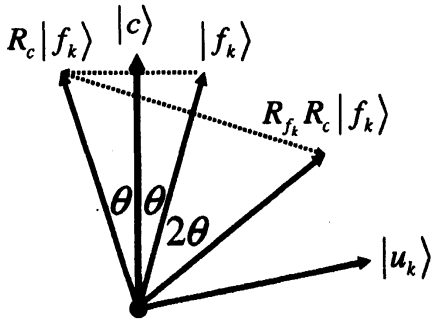


Figure 4: Reflection operators

We now describe our quantum algorithm for any EOIP as follows.

**Quantum Algorithm for EOIP**

(1) Create the oracle state $|f_k\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f_k(x)}|x\rangle$ by $O_{f_k}$.
(2) If $\cos^2\phi \geq \cos^2\theta$, perform Steps from (3) to (5). Otherwise, measure $U|f_k\rangle$ and output the result, where $U$ is the unitary operator given in Lemma 2.2.
(3) Perform Step (4) $l_0 = \lceil \frac{\arccos(1/\sqrt{N})}{2\theta} - \frac{1}{2} \rfloor$ times. Let $|f_k^{(0)}\rangle = |f_k\rangle$ be the initial state and $|f_k^{(l)}\rangle$ be the state obtained after the $l$-th repetition.
(4) Apply the reflection operators $R_c$ and $R_{f_k}$ to $|f_k^{(l)}\rangle$. Then, we obtain $|f_k^{(l+1)}\rangle = R_{f_k} R_c |f_k^{(l)}\rangle$.
(5) Measure the state $U|f_k^{(l_0)}\rangle$ and output the result.

It is easy to analyze the number $l_0$ of queries in this algorithm. Since $\sin\theta \leq \theta$, $\arccos(1/\sqrt{N}) < \pi/2$ and $\sin\theta = \sqrt{1 - \langle c|f_k\rangle^2} = \sqrt{(1-(1/N))(1-\sigma)}$, this algorithm needs at most $\lceil \frac{\pi}{\sqrt{(1-(1/N))(1-\sigma)}} \rceil = O((1-\sigma)^{-1/2})$ queries.

Now, we consider the success probability of the above algorithm. In the case that $\cos^2\phi \geq \cos^2\theta$, the success probability is $\cos^2\phi = \Omega(1-\sigma)$ by Lemma 2.2. In the other case, the angle between $|c\rangle$ and $|f_k^{(l_0)}\rangle$ becomes $(2l_0+1)\theta$ by the reflection operators after $l_0$ repetitions of (4). We then have $|(2l_0+1)\theta - \arccos(1/\sqrt{N})| \leq \theta$, which implies that the angle between $|f_k^{(l_0)}\rangle$ and $|u_k\rangle$ is at most $\theta$. We therefore obtain $|\langle f_k^{(l_0)}|u_k\rangle|^2 \geq \cos^2\theta = \Omega(\sigma)$ by Lemma 2.2. □

### 2.2 Approximated Equianguler Case

We extend the equiangular case to a slightly general case according to the same geometric intuition with an argument called "pretty good measurement" of the quantum information theory for designing orthonormal basis $\{u_i\}_i$.

**Theorem 2.4** There exists a quantum algorithm that solves any OIP satisfying $\mathrm{rank}((|f_0\rangle \cdots |f_{N-1}\rangle)) = N$, $c\sigma \leq \langle f_k|f_l\rangle \leq \sigma$ for any distinct $k$ and $l$ and any constant $0 < c < 1$ using $O((1-\sigma)^{-1/2})$ queries with a constant probability.

**Proof.** In the previous equiangular case, we can easily obtain the optimal unitary operator $U$ for maximizing the success probability by the exact equiangularity. On the other hand, we have to need to design "good" orthonormal basis $\{u_i\}_i$ and analyze the success probability in more general case. The following technical lemma gives the good orthonormal basis to construct the desired unitary operator based on the argument of the so-called pretty good measurement.

**Lemma 2.5** Assume that the rank of $F = (|f_0\rangle \cdots |f_{N-1}\rangle)$ is equal to $N$. There exists a unitary operator $U = (|u_0\rangle \cdots |u_{N-1}\rangle)^\dagger$ such that the success probability of obtaining $k$ by measuring $U|f_k\rangle$ in the computational basis is at least $1 - \sigma_{\max}$, where $\max_{i \neq j} |\langle f_i|f_j\rangle|$, i.e., $|\langle k|U|f_k\rangle|^2 \geq 1 - \sigma_{\max}$.

**Proof.** Let $G = F^\dagger F$ be the $N \times N$ Gram matrix for $F$ and let $U = (|u_0\rangle \cdots |u_{N-1}\rangle)$ be any $N$-dimensional unitary matrix. Note that the $(i,j)$ entry of the matrix $UF$ is $\langle u_i|f_j\rangle$ The success probability by measuring $U|f_k\rangle$ in the computational basis is then $|\langle k|U|f_k\rangle|^2 = |\langle u_k|f_k\rangle|^2 = |\langle k|UF|k\rangle|^2$. By the singular-value decomposition, the matrix $F$ can be described as the form of $F = P^\dagger T Q$, where $P$ and $Q$ are unitary matrices and $T$ is the diagonal matrix of $\mathrm{diag}(\sqrt{\lambda_0} \cdots \sqrt{\lambda_{N-1}})$, where $\lambda_i$ is the eigenvalue of the Gram matrix $G = F^\dagger F$. Note that every $\lambda_i$ is a non-zero real number since $G$ is a real symmetric matrix and $\mathrm{rank}(G) = N$. Therefore the success probability is $|\langle k|UP^\dagger TQF|^2$. By setting $U = Q^\dagger P$, the success probability is $|\langle k|Q^\dagger TQF|^2 \geq \min_i\{|\lambda_i|\}$, i.e., the success probability is lower bounded by the minimum singular value $|\lambda_{\min}| = \min_i\{|\lambda_i|\}$ of the Gram matrix $G$.

We now evaluate a lower bound of $|\lambda_{\min}|$. By the property of the minimum singular value of a real symmetric matrix, we have $|\lambda_{\min}| = \min_{|\phi\rangle\in\mathbb{R}^N,\||\phi\rangle\|=1} |\langle\phi|G|\phi\rangle|$. Now letting $|\phi\rangle = \sum_i \alpha_i|\phi\rangle$ ($\alpha_i \in \mathbb{R}$, $\sum_i |\alpha_i|^2 = 1$),

$$\begin{aligned}
\min_{|\phi\rangle\in\mathbb{R}^N,\||\phi\rangle\|=1} |\langle\phi|G|\phi\rangle| &= \min_{|\phi\rangle\in\mathbb{R}^N,\||\phi\rangle\|=1} \Bigg| 1-\sigma_{\max} + \sum_{i<j,G_{i,j}\geq 0} (\sigma_{\max}\alpha_i^2 + 2|G_{i,j}|\alpha_i\alpha_j + \sigma_{\max}\alpha_j^2) \\
&\qquad + \sum_{i<j,G_{i,j}<0} (\sigma_{\max}\alpha_i^2 - 2|G_{i,j}|\alpha_i\alpha_j + \sigma_{\max}\alpha_j^2) \Bigg| \\
&= \min_{|\phi\rangle\in\mathbb{R}^N,\||\phi\rangle\|=1} \Bigg| 1-\sigma_{\max} + \sum_{i<j,G_{i,j}\geq 0} (|G_{i,j}|(\alpha_i+\alpha_j)^2 + (\sigma_{\max}-|G_{i,j}|)(\alpha_i^2+\alpha_j^2) \\
&\qquad + \sum_{i<j,G_{i,j}<0} (|G_{i,j}|(\alpha_i-\alpha_j)^2 + (\sigma_{\max}-|G_{i,j}|)(\alpha_i^2+\alpha_j^2) \Bigg| \\
&\geq 1-\sigma_{\max}.
\end{aligned}$$

This completes the proof of the lemma. □

Now, we describe the quantum algorithm for the general case. This algorithm has the almost same structure as the previous one. We also make use of the following two reflection operators $R_{f_k} = 2|f_k\rangle\langle f_k| - I$ and $R_c = 2|c\rangle\langle c| - I$ in this algorithm, where $|c\rangle$ is the mean state among $|f_0\rangle, ..., |f_{N-1}\rangle$. Recall that $\sigma_{\max} = \max_{i\neq j} |\langle f_i|f_j\rangle|$.

**Quantum Algorithm for Approximated EOIP with** rank($N$)

(1) Create the oracle state $|f_k\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f_k(x)}|x\rangle$ by $O_{f_k}$.

(2) If $\sigma_{\max} < c_0$ for a fixed constant $c_0 > 0$, perform Steps from (3) to (5). Otherwise, measure $U|f_k\rangle$ and output the result, where $U$ is the unitary operator given in Lemma 2.5.

(3) Perform Step (4) $l_0 = \lceil \frac{\pi}{4 \arccos \sigma_{\max}} \rfloor$ times. Let $|f_k^{(0)}\rangle = |f_k\rangle$ be the initial state and $|f_k^{(l)}\rangle$ be the state obtained after the $l$-th repetition.

(4) Apply the reflection operators $R_c$ and $R_{f_k}$ to $|f_k^{(l)}\rangle$. Then, we obtain $|f_k^{(l+1)}\rangle = R_{f_k} R_c |f_k^{(l)}\rangle$.

(5) Measure the state $U|f_k^{(l_0)}\rangle$ and output the result.

One can easily see that the query complexity of this algorithm is at most $O(\sqrt{1-\sigma_{\max}})$. We can also show that this algorithm has a constant success probability by the property of the orthogonal basis $\{u_i\}_i$. □

## 3 Lower Bounds

The upper bounds given by the previous algorithms are actually optimal. We show a matching lower bound of a specific OIP parametrized by the inner product. Let $\sigma_{max}$ be the maximum inner product of two oracle states in $S = \{f_0, \cdots, f_n\}$ for a specific OIP. Then the following can be seen easily.

**Theorem 3.1** There exists a specific OIP that needs $\Omega(\frac{1}{\sqrt{1-\sigma_{max}}})$ queries.

**Proof.** We show that $\Omega(\frac{1}{\sqrt{1-\sigma_{max}}})$ queries are necessary to solve OIP for the so-called hybrid oracles [1]. Consider the function with two parameters $k$ and $i$, $f_{k,i} : \{0,1\}^n \to \{0,1\}$ as follows: let $i = (i_1, i_2, \ldots, i_{n-k}, i_{n-k+1}, \ldots, i_n)$ and $x = (x_1, x_2, \ldots, x_{n-k}, x_{n-k+1}, \ldots, x_n)$. then $f_{k,i}(x) = 1$ iff (i) $(i_1, ..., i_{n-k}) = (x_1, ..., x_{n-k})$ and (ii) $(i_{n-k+1}, ..., i_n) \cdot (x_{n-k+1}, ..., x_n) = 0 \pmod 2$.

Then $OIP_k$: $s = \{f_{k,0}, \cdots, f_{k,n}\}$ needs $\Omega(\sqrt{N/2^k})$ queries by Theorem 7 in [1], where $N = 2^n$ since the values of $f_{k,i}(x)$ and $f_{k,j}(x)$ differ from each other for at least $2^k/2$ different $x$, $\sigma_{max}$ can be written as $\frac{1}{N}(N - \frac{2^k}{2} - \frac{2^k}{2}) = 1 - \frac{2^k}{N}$. Therefore, the above lower bound can be rewritten as $\Omega(\sqrt{N/2^k}) = \Omega(\frac{1}{\sqrt{1-\sigma_{max}}})$ queries as desired. □

## 4 Open Problems

We gave upper and lower bounds of OIPs in which every distinct pair of oracle state has the almost same inner product. An open problem is to find a simple quantity for characterization of the query complexity of an arbitrary $N \times N$ OIP (more generally, $M \times N$ OIP for $M > N$), which might not be the inner product. Also, we might able to characterize classical query complexities, which is related with the exact learning in computational learning theory, by our geometrical intuition. It would be interesting if we can obtain a unified geometrical view of classical and quantum query complexities for general OIPs.

## References

[1] A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R. H. Putra, and S. Yamashita. Quantum identification of boolean oracles. In *Proceedings of the 21st Annual Symposium on Theoretical Aspects of Computer Science*, LNCS 2996, pages 105–116, 2004.

[2] A. Ambainis, K. Iwama, A. Kawachi, R. H. Putra, and S. Yamashita. Robust quantum algorithms for oracle identification. quant-ph/0411204, 2005.

[3] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[4] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th ACM Symposium on Theory of Computing*, pages 212–218, 1996.

[5] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.